

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA)	
)	
v.)	
)	Criminal No. 09CR10382-DPW
ALBERT GONZALEZ)	
)	<u>FILED UNDER SEAL</u>
Defendant.)	

**GOVERNMENT’S RESPONSE TO MOTION TO INTERVENE
FOR THE PURPOSE OF SEEKING A PROTECTIVE ORDER**

J C Penney, “Company A” in the Indictment in this case, has moved to intervene for the purpose of seeking a Court order barring the U.S. Attorney’s Office from public compliance with Fed. R. Crim. P. 12.4 and its analogue Local Rule 112.4 of this Court. The order presumably would also extend to restraining otherwise public filings with this Court concerning sentencing in this matter. In both respects, J C Penney seeks to bar disclosure by the government of independently obtained information. The United States does not object to their intervention for the limited purpose of airing this issue. It does object to the order which J C Penney seeks.

There is a strong presumption in this District of public disclosure in charged criminal cases of significant information relating to the charges in an Indictment. In the case of computer attacks such as the one charged here, the argument for this is undeniably strongest when people’s credit or debit card numbers are known, with certainty, to have been stolen from a corporation. However, it is only marginally less so when people’s credit or debit card numbers are put at risk by the failure of a corporation’s protective system. When a fraud or Internet attack has compromised a corporation’s security system and potentially put customers’ credit or debit card

numbers at risk, it is far fairer for their customers to evaluate that risk on a fair presentation of the facts than for the corporation, alone, to be told of the intrusion by the government.

J C Penney's case falls within the second category. The Secret Service went to J C Penney with the information and evidence that its computer system, used to process payment card transactions, had been broken into.¹ Although the protective system used by J C Penney had unquestionably failed, the Secret Service had no evidence as to whether payment card numbers had been stolen.

Our presumption of public disclosure in charged criminal cases does not depend on the costly proof of evidence of negligence by the corporation, which we rarely can obtain, and then only with the full cooperation and guidance of the company. Most people want to know when their credit or debit card numbers may have been put at risk, not simply if, and after, they have clearly been stolen. The presumption of disclosure has an additional significant benefit, though, besides the right of the card holder to know when he has been exposed to risk. Knowing that card holders will be concerned whenever their credit or debit card information is put at risk, if they know of it, provides an incentive to companies to invest in the protections their customers would want. Transparency makes the market work in this area.

Of course, there can be countervailing reasons, though ones often limited in duration, for anonymity. By way of example only, when there has been a successful fraud or Internet attack, businesses may need a period of time to ensure the security failings which permitted the crime

¹ Attached are excerpts of instant messaging communications between defendant Albert Gonzalez and fugitive defendant Hacker 1 in this case discussing the conspirators' activities within JCP's (J C Penney's) computer network during the winter of 2007/2008. They are attached for the limited purpose of more fully responding to J C Penny's Motion, and not offered as against defendant Gonzalez at this time.

have been fully identified and corrected. Independently, a period of confidentiality may be necessary for effective investigation of the criminal conduct. None of the reasons now stated by J C Penney for making an exception to transparency in this case are persuasive.

In this case, New Jersey indicated that it would apply a different policy while the case remained in their hands, but made no commitment that J C Penney's name would never be disclosed in the course of litigation there or elsewhere. J C Penney's established counsel knew that New Jersey would not and could not impose its policy decision on another district without the approval of the Department of Justice in Washington. A case may begin in a jurisdiction without this presumption, as it did in New Jersey in this case. Then it can move to a jurisdiction with this presumption, such as Massachusetts, for any one of a number of reasons. So long as the company hasn't relied to its detriment on the practices of the first district—and there is no meaningful detrimental reliance here—the policies and accountability of the district handling the case necessarily prevail.

There is also a presumption of transparency in this judicial district that applies to corporations which have been the victims of fraud or abuse. It begins with the Fed. R. Crim. P. 12.4/Local Rule 112.4 submission which serves not only to alert the Court of possible grounds for disqualification, but also to enable the public to independently make this evaluation, furthering the judicial system's efforts towards transparency. Needless to say, the fact that a case began in another district, does not affect the application of the rule here.

Conclusion

CBS News.com already has identified J C Penney as one of the unnamed corporations in

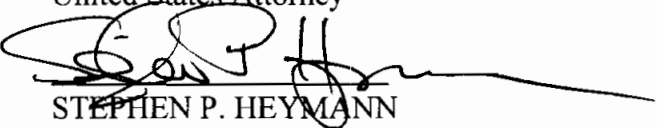
the Indictment, greatly diminishing J C Penney's interests here.² It would be perfectly appropriate for them to make a public statement that there is no evidence that any credit or debit cards were stolen. The government could also amend its Rule 12.4/112.4 disclosure to separate those companies with respect to which there is evidence that payment card data was stolen and those with respect to which there is not.

However, the unquestioned object of the computer attack on J C Penney was innumerable credit and debit card holders and the primary impact was to put them at risk. J C Penney was, as it claims, a secondary victim, but that does not entitle it to hide from the primary victims the facts enabling them to understand and assess the risks to which they were exposed.

The Court should grant J C Penney's limited motion to intervene, but deny the protective order they seek.

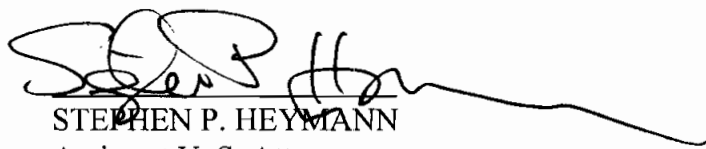
Respectfully submitted,
CARMEN M. ORTIZ
United States Attorney

By:


STEPHEN P. HEYMANN
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document, and the accompanying Limited Motion to Seal, is being sent by electronic mail to Martin Weinberg, attorney for Albert Gonzalez, and Michael Ricciuti, attorney for J C Penney.


STEPHEN P. HEYMANN
Assistant U. S. Attorney

Date: December 29, 2009

² A printout of the article from the CBS News.com website is attached.

ATTACHMENT A

ICQ instant messaging logs were recovered from one of Albert Gonzalez's laptop computers. In the following excerpts from those logs, ICQ number 372712 is the defendant identified as "Hacker 1" in the Indictment and ICQ number 324321 is defendant Albert Gonzalez. "Hacker 2" has been substituted where Hacker 2's online pseudonym appears in the original text. Both Hacker 1 and Hacker 2 are still being sought by law enforcement authorities. Portions of the 12/16/2007 exchange have been redacted, where indicated.

Structured Query Language ("SQL") is a computer programming language designed to retrieve and manage data on computer databases. "SQL Injection Attacks" are methods of hacking into and gaining unauthorized access to computers connected to the Internet. In the excerpts below, "pw" is believed to be the abbreviation for password(s).

324321:11/1/2007 7:50:38 PM
have you done any work on jcp?

372712:11/1/2007 7:51:13 PM
i personally didnt, hacker 2 just scanned few sqls for weak pw

324321:11/1/2007 7:52:12 PM
i thought jcp was inject

372712:11/1/2007 7:52:29 PM
yes i mean he scanned inside

372712:11/1/2007 7:52:37 PM
i hacked jcp with injection too

372712:11/1/2007 7:53:26 PM
they have most of ports open wasnt too hard

324321:11/4/2007 8:04:01 PM
what did hacker 2 say about jcp?

372712:11/4/2007 8:04:40 PM
he hacked 100+ sqls inside and stopped

"Sniffer" programs are used to monitor and capture data moving across a computer network. "Dumps" are a slang term for track 2 data, the data recorded on the magnetic stripes on the backs of credit and debit cards.

372712:12/16/2007 3:31:45 PM

hacker 2 told me he found a place to sniff for dumps in jcp

3727 2:

12/16/2007 3:36:01 PM

i see, hacker 2 showed you anything?

3727 2:

12/16/2007 3:36:19 PM

JCP-J98 A..??..hIPCRED98O?8U\S?...T10014.I000COLJ wa.....[REDACTED]/LISA A
^49127010[REDACTED]0000000000000

JCP-J98 A..??..hIPCRED98O?8U\S?...T10014.I000COLJ [RECACTED]/LISA A
^4912701[REDACTED]0000000000

324321:12/16/2007 3:36:19 PM

nope, when did hacker 2 have this news?

3727 2:12/16/2007 3:36:30 PM

yesterday?

324321:12/16/2007 3:38:19 PM

hmm, where is track2?

3727 2:12/16/2007 3:39:42 PM

hm yea, maybe he didnt send me full log

324321:12/16/2007 3:39:59 PM

im curious how hacker 2 moved around on jcp so quickly w/o making noise

372712:12/16/2007 3:40:59 PM

sql servers is his key to everything heh

324321:12/24/2007 3:38:20 PM

i got access to the jcp pos network :)

3727 11/3/17/2008 7:25:10 PM
how are things ended with JCP?

3243 11/3/17/2008 7:25:53 PM
i stopped bruting the domain admin pw

3243 11/3/17/2008 7:26:01 PM
after hacker 2 got domain admin i stopped

ATTACHMENT B

December 11, 2009

Retailer Wants Breach Kept Secret

Retail Realities: Major Chain Wants Court To Protect Its "Dignity," Keep Shareholders In The Dark

Like this Story? Share it:



Share



(CBS)

(CBS) This column was written by Evan Schuman, the editor of StorefrontBacktalk, a site that tracks retail technology, e-commerce and security issues. Retail Realities appears every Friday. Evan can be reached at e-mail and on Twitter.

Albert Gonzalez—who has already pleaded guilty to masterminding a cyberthief ring that stole data from TJX, BJ's Wholesale Club, Boston Market and Sports Authority, among other major chains—signed papers this month agreeing to plead guilty to the remaining federal charges against him. But one of the retail chain victims, which federal officials have yet to officially identify, asked the court to protect its "dignity" by preventing the government from releasing the chain's name.

Gonzalez agreed to plead guilty to his role in attacks on Heartland, Hannaford and 7-Eleven in a document signed at 10:14 AM New York time on Dec. 2. In a very related matter, a federal judge on Monday (Dec. 7) dismissed a data breach-related lawsuit against Heartland Payment Systems, saying that the plaintiffs hadn't proved any of their allegations that Heartland knew it had inadequate security and lied about it to shareholders.

The document that Gonzalez signed also ordered the case transferred out of Camden, N.J., and merges it with similar charges in Boston, according to a copy of the Consent to Transfer of Case for Plea and Sentence filing. (That's the document's actual name. It's good to see that the Justice Department isn't wasting taxpayer dollars on a good copyeditor.) No details of the plea agreement were filed as of late Wednesday (Dec. 9).

One of the more interesting parts of this case has been that at least three retail chain victims in the Gonzalez attacks have remained unidentified-on the record, at least-by federal officials. Published reports have identified Target and J.C. Penney as two of those mystery merchants. But last month, one of those chains quietly had a lawyer ask U.S. District Court Judge Jerome B. Simandle, sitting in Camden, to keep a lid on the chain's identity.

Attorney Kevin G. Walsh, who identified his client solely as "Company A," asked Simandle for a protective order to "ensure the preservation of (the major retailer's) dignity, privacy and anonymity."

The letter relied on provisions in the Crime Victims Rights Act. There's something unsettling about equating the victim of a rape or a mugging who should be spared the public humiliation of the crime with a multi-billion-dollar chain's efforts to keep a major data breach secret from its shareholders and customers. How does a department store preserve its "dignity" (borrowing the word from the letter)? When the victim is a publicly held corporation that asks consumers to trust it with various forms of payment cards, should a federal judge sanction those secrecy efforts?

Although not mentioned in this filing, there is one legitimate reason to maintain secrecy, and that's security. If the details of the breach would reveal security holes that still exist, a legitimate argument could be made to keep either those details or the retailer's name quiet for a brief period. The only problems are that these breaches occurred several years ago and those holes have presumably been plugged long ago. Indeed, if they have yet to be plugged, I'm not so sure that that retailer doesn't deserve whatever exposure the public filing would deliver.

The mystery merchant's concerns may be alleviated by Gonzalez's guilty plea, but perhaps not. The fear had always been that a trial would not only force the disclosure of all the retail victims' names but also reveal quite a bit about how weak their security was at the times of the attacks. A guilty plea doesn't necessary make that all go away, as attorneys involved in the case might feel comfortable discussing the victims after the case has been resolved. But a federal protective order would certainly help keep those shareholders and customers in the dark.

By Evan Schuman
Special to CBSNews.com